REMARKS

Claims 29-54 were pending prior to this Amendment. In the Office Action mailed January 10, 2008, the Examiner rejected claims 29-54 under section 103 as being unpatentable over Cheline (US PGPUB No. 2003/0041136) in view of Nguyen (US PGPUB No. 2003/0172145).

The Examiner also rejected claims 36, 47 and 53 under section 112 as failing to comply with the written description requirement based on the Examiner's assertion that there is no disclosure in the specification or original claims for the claim limitation that "software is adapted to inhibit modification of the software by the user."

The Examiner also rejected claims 49-52 under section 112 based on the Examiner's assertion that the term "a computer readable medium" lacks antecedent basis.

No claim stands rejected under section 102 for anticipation.

In this Amendment, Applicants have cancelled claims 49-54. Applicants have amended claims 31 and 47 to correct grammatical issues. Applicants have added claims 55-56 to claim additional subject matter to which Applicants are entitled.

Substance of Interview (MPEP 713.04)

A telephonic interview was conducted on February 12, 2008. Examiner Johnson, Examiner Moazzami and Applicants' attorney, Scot Reader, participated.

Applicants thank the Examiners for their participation in the interview.

Independent claims 29, 30 and 36 were discussed in the interview. With regard to claim 29, Applicants stressed that Cheline does not disclose the claim recitation of preventing detected attempted writes to permanent memory on an end system while the end system is permitted access to a VPN. With regard to claim 30, Applicants stressed that Cheline does not disclose the claim recitation of redirecting to temporary memory on an end system detected attempted writes to permanent memory on the end system while the end system is permitted access to a VPN. Applicants also stressed differences between the inventive goals of Cheline and Applicants' invention that help explain why Cheline would not address these claim recitations, for example, Cheline is concerned with VPN configuration and data privacy whereas Applicants' invention is directed at preventing an end system accessing a VPN from becoming permanently infected by malicious code, even where the end system becomes temporarily infected while accessing the VPN. With regard to claim 36, Applicants stressed that the claim limitation of software adapted to inhibit modification of the software by the user has support in the original specification at p.3, lines 15-17, p.4, lines 11-15 and p.8, lines 6-8.

Section 112 Rejections

The Examiner rejected claims 36, 47 and 53 under section 112 as failing to comply with the written description requirement based on the Examiner's assertion that there is no disclosure in the specification or original claims for the claim recitation of software adapted to inhibit modification of the software by the user.

Applicants respectfully submit that the Examiner is mistaken about the scope of Applicant's disclosure and request reconsideration of this section 112 rejection. At p.8, lines 6-8 of Applicants' original specification, it is stated: "Software 300 is embedded prior to delivery of end system 20 to the remote worker and provides no interface for modification by the remote worker." Moreover, at p.3, lines 15-17, it is

8

stated: "[T]he operating software is configured without support for drivers or user-attached peripherals, such as hard disk drives, that could create new vulnerabilities." Furthermore, at p.4, lines 11-15, it is stated: "Since the end system's operating software is embedded in a nonvolatile memory and made unsupportive of user-attached peripherals ... the end system is made virtually impervious to permanent infection by malicious code." The claim recitation of software adapted to inhibit modification of the software by the user therefore finds support at numerous places in the original specification, and the section 112 rejections of claims 36, 47 and 53 are traversed.

The Examiner also rejected claims 49-52 under section 112 based on the Examiner's assertion that the term "a computer readable medium" lacks antecedent basis. Applicants have cancelled claims 49-52 to obviate these section 112 rejections.

Section 103 Rejections

Of the independent claims pending prior to this Amendment, claims 29 and 42 remain. Applicants respectfully submit that the combination of Cheline and Nguyen relied on by the Examiner for his section 103 rejection of these independent claims fails to teach or suggest certain elements recited in these claims. Moreover, claims 30, 36, 43 and 47 that depend from claims 29 and 42 recite additional elements that are not taught or suggested by the combination.

Applicants begin by reiterating a significant goal of their invention that is not shared by Cheline or Nguyen and illuminates why Cheline and Nguyen do not address certain recitations found in Applicants' claims. This unique goal of Applicants' invention is preventing permanent infection by malicious code of an end system that becomes temporarily infected while accessing a VPN, and is achieved by write-protecting the

permanent memory while the end system accesses the VPN. As stated at p.3 of Applicants' specification, starting at line 5:

> In one aspect, a VPN capable end system is made virtually impervious to permanent infection. The end system has a nonvolatile memory, such as a flash memory, in which all of the end system's operating software is embedded and from which it is booted. The nonvolatile memory is effectively write-protected so as to render it invulnerable to malicious code. Particularly, while connected to the VPN, the end system is configured to direct all data writes to the end system to a writable memory, such as a RAM disk. Moreover, the end system is configured to purge the writable memory when the VPN connection is terminated so as to render the acquisition of any malicious code thereon temporary.

This effective write-protection of permanent memory while the end system accesses the VPN is achieved, in part, by:

- Preventing detected attempted writes to a permanent memory of an end system while the end system accesses a VPN, as recited in claims 29 and 42;
- Redirecting to a temporary memory of the end system detected attempted writes to the permanent memory while the end system accesses a VPN, as recited in claims 30 and 43; and
- Adapting software embedded in the permanent memory to inhibit modification of the software by the user of the end system, as recited in claims 36 and 47.

By preventing writes to the permanent memory by either a user of the end system or a server-side system to which the end system is connected on a VPN, permanent infection of the end system is advantageously avoided even in the event the end

system becomes temporarily infected while interfacing with the end system user or server-side system.

The combination of Cheline and Nguyen does not teach or suggest the mentioned claim elements. Indeed, the primary reference relied on by the Examiner, Cheline, allows its permanent memory (flash memory 234) to be written by both client- and server-side systems. For example, at paragraph [0057] of Cheline it is stated: "The flash memory 234 is a type of constantly-powered nonvolatile memory that can be erased and reprogrammed in units of memory called blocks." Thereafter, Cheline describes multiple instances of writing the flash memory by a client computer and VPN service provider. At paragraph [0063] of Cheline, it is indicated that the user of one of client computers and the modem receive from a VPN service provider a one-time only password that is stored in the flash memory. At paragraph [0064] of Cheline, it is indicated that the modem further receives from a VPN service provider VPN security policies, a private key and certificate, and a root CA certificate that are stored in the flash memory. And at paragraph [0067] of Cheline, it is indicated that the modem receives from a client computer upon requesting initiation of a VPN session a MAC address and/or IP address that is/are stored in the flash memory. Accordingly, far from write-protecting its permanent memory, Cheline includes explicit teachings to allow its permanent memory to be written by network devices, leaving its VPN platform vulnerable to permanent infection.

Reasons for allowability of the claims over the combination of Cheline and Nguyen are now discussed in even greater detail.

11

1. Claims 29-48 Are Allowable over Cheline and Nguyen Since The Combined References Do Not Teach Preventing Detected Attempted Writes to Permanent Memory on an End System While the End System is Permitted VPN Access

Independent claims 29 and 42 recite preventing detected attempted writes to permanent memory on an end system while the end system is permitted VPN access. Applicants respectfully submit that the Examiner is mistaken in his view that Cheline addresses this claim recitation and request reconsideration.

The Examiner describes his rejection of claim 29 at p.8 of the Office Action. There, in asserting correspondence for the above claim recitation, the Examiner states that while permitting VPN access "Cheline discloses attempted writes to the end system and preventing detected attempted writes to permanent memory on the end system." However, the Examiner provides no citation for the asserted correspondence. The Examiner later discusses his rejection of claim 42 at pp.14-15 of the Office Action. There, asserting correspondence for the above claim recitation, the Examiner states that while permitting VPN access "Cheline discloses attempted writes to the end system and preventing detected attempted writes to the permanent memory. (see Cheline paragraph [0049], lines 11-14: permit access (encrypted packets transferred) to end system)."

Accordingly, the Examiner apparently finds alleged correspondence for the recitation of preventing detected attempted writes to permanent memory on an end system while the end system is permitted VPN access at paragraph [0049] of Cheline at lines 11-14 which states that "encrypted packets can be communicated between a client computer and the server-side system" on a VPN connection.

The Examiner's view that communicating encrypted packets to an end system teaches preventing detected attempted writes to permanent memory on the end system is

mistaken. Applicants' do agree with the Examiner that "placement of transferred information on [an] end system enables writing" (Office Action, p.10). Applicants' also acknowledge that Cheline discloses a permanent memory (e.g. flash memory 234) and a temporary memory (e.g. cache 236). While these facts are not in dispute, however, they do not amount to a teaching of preventing detected attempted writes to a permanent memory on an end system. Mere receipt of encrypted packets on an end system and the presence of a permanent memory on the end system[1] do not imply an attempt to write such permanent memory or that any such attempt is detected and prevented. In Cheline's system, the received encrypted packets could be written to temporary memory (e.g. cache 236); or could be written to permanent memory without prevention (e.g. flash memory 234), for example.

Based on the foregoing, independent claims 29 and 42 are allowable, and since all claims 30-41 and 43-48 depend thereon, these claims are also allowable. If the Examiner persists in his rejection of claims 29 and 42, Applicants respectfully request that the Examiner explain with greater precision how mere receipt of encrypted packets on an end system and the presence of a permanent memory on the end system fairly teach or suggest preventing detected attempted writes to the permanent memory.

---

[1] Applicants note that the permanent memory in Cheline relied on by the Examiner for his rejection is not even on an end system, but rather on a modem 106 that is interposed between a client computer 102 and server-side systems 130, 146. Cheline teaches away from putting VPN client software on an end system, stating: "[T]he VPN system disclosed herein is relatively easy for telecommuting users to install and maintain, as the client VPN software resides on the user's modem instead of the user's client computer. This alleviates drawbacks associated with software interoperability and maintenance issues on the user's client computer." [0028].

2. Claims 30 and 43 Are Allowable over Cheline and Nguyen for the Additional Reason That the Combined References Do Not Teach Redirecting to Temporary Memory on an End System Detected Attempted Writes to Permanent Memory on the End System While the End System is Permitted VPN Access

Claims 30 and 43 recite or incorporate redirecting to a temporary memory on an end system detected attempted writes to a permanent memory on the end system while the end system is permitted VPN access. Applicants respectfully submit that the Examiner is mistaken in his view that Cheline addresses this claim recitation and request reconsideration.

The Examiner describes his rejection of claims 30 and 43 at p.10 of the Office Action. There, in asserting correspondence for the above claim recitation, the Examiner states that "Cheline discloses the method, end system medium of claims 29, 42 ..., wherein the step of attempted writes to the end system further comprises redirecting to temporary memory detected attempted writes to permanent memory. (see Cheline paragraph [0049], lines 11-14: transfer of information between VPN connected systems (placement of transferred information on end systems enables writing); paragraph [0047], lines 1-10; paragraph [0058], line 1: permanent type or temporary memory utilized, placement of information within temporary or permanent memory)."

Accordingly, the Examiner finds correspondence for the recitation of redirecting to a temporary memory on an end system detected attempted writes to a permanent memory on the end system while the end system is permitted VPN access at paragraph [0049] of Cheline at lines 11-14, paragraph [0047] lines 1-10, and paragraph [0058] line 1. Paragraph [0049] at lines 11-14 discusses communication of encrypted packets on a VPN connection. Paragraph [0047] and [0058] indicate that Cheline's modem has both a permanent memory (e.g. flash memory 234) and a

temporary memory (e.g. cache 236). Thus, these citations do not teach beyond what has been discussed in relation to claims 29 and 42, namely, (1) receipt of encrypted packets by an end system on a VPN connection, (2) a permanent memory and (3) a temporary memory.

The Examiner's view that communicating encrypted packets to an end system teaches redirecting to a temporary memory on an end system detected attempted writes to a permanent memory on an end system is mistaken. While Applicants' agree with the Examiner that "placement of transferred information on [an] end system enables writing" (Office Action, p.10) and acknowledge that Cheline discloses a permanent memory (e.g. flash memory 234) and a temporary memory (e.g. cache 236), this does not amount to a teaching of redirecting to a temporary memory detected attempted writes to a permanent memory. In Cheline's system, information in received encrypted packets could be written to permanent memory (e.g. flash memory 234); or could be written to temporary memory (e.g. cache 236) without redirection, for example.

Applicants note that an online technical dictionary defines "redirect" as "to change the direction or course of" (http://www.answers.com/topic/redirect?cat=technology). There is no teaching in Cheline or Nguyen to change the direction or course of an attempted write of permanent memory so that temporary memory is written instead. This is a highly unusual feature of Applicants' invention that furthers Applicants' goal of preventing permanent infection by malicious code of an end system that becomes temporarily infected while accessing a VPN.

The absence from Cheline of any teaching or suggestion of redirecting to temporary memory attempted writes to permanent memory provides an independent reason that claims 30 and 43 are allowable. If the Examiner persists in his rejection of claims 30 and 43, Applicants respectfully request that the Examiner explain with greater particularity how the mere receipt of encrypted packets on an end system and the

15

presence of a permanent and temporary memory teach or suggest redirecting to the temporary memory attempted writes to the permanent memory.

3. Claims 36 and 47 Are Allowable over Cheline and Nguyen for the Additional Reason That the Combined References Do Not Teach Software Embedded in a Permanent Memory on a VPN Capable End System that is Adapted to Inhibit Modification of the Software by the User

Claims 36 and 47 recite or incorporate software embedded in a permanent memory on a VPN capable end system that is adapted to inhibit modification of the software by a user of the end system. Applicants respectfully submit that the Examiner is mistaken in his view that Cheline addresses this claim recitation and request reconsideration.

The Examiner describes his rejection of claims 36 and 47 at p.12 of the Office Action. There, in asserting correspondence for the above claim recitation, the Examiner states that "Cheline discloses the method, end system medium of claims 35, 42 ..., wherein the software is adapted to inhibit modification of the software by the user. (see Cheline paragraph [0046], lines 1-4; paragraph [0047], lines 6-10: software, program products, operating system software, perform functions; page 11, claim 13: computer-readable medium)."

The cited paragraphs do not teach or suggest software embedded on a permanent memory of a VPN capable end system wherein the software is adapted to inhibit modification of the software by a user of the end system. While Cheline mentions at paragraph [0047] an embedded operating system on memory 210, there is no indication in any of the cited paragraphs that the embedded operating system is adapted to inhibit its modification by a user of an end system. For example, there is no indication to configure the embedded operating system without support for drivers or user-attached peripherals. The absence from Cheline of software embedded in

permanent memory adapted to inhibit its modification by a user of a VPN capable end system provides an independent reason that claims 36 and 47 are allowable.
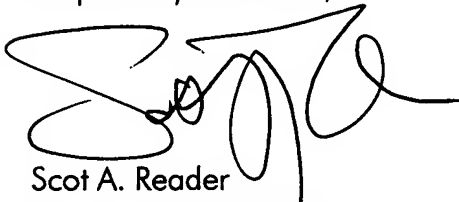
4. New Claims 55 and 56 Are Allowable

Claims 55 and 56 have been added to claim additional subject matter that defines over Cheline and Nguyen. Claim 55, on which claim 56 depends, addresses a VPN-capable end system having a plurality of memories consisting of at least one write-protected permanent memory and at least one temporary memory. Naturally, use of the transitional phrase "consisting of" requires write-protection of the entire permanent memory on the VPN-capable end system recited in claim 55. See MPEP 2111.03. In contrast to what is recited, Cheline allows writing of a permanent memory (flash memory 234) by both client- and server-side systems. For example, at paragraph [0057] of Cheline it is stated: "The flash memory 234 is a type of constantly-powered nonvolatile memory that can be erased and reprogrammed in units of memory called blocks." Thereafter, multiple instances of writing the flash memory by a client computer and VPN service provider are described. At paragraph [0063] of Cheline, it is indicated that the user of one of client computers and the modem receive from a VPN service provider a one-time only password that is stored in the flash memory. At paragraph [0064] of Cheline, it is indicated that the modem further receives from a VPN service provider VPN security policies, a private key and certificate, and a root CA certificate that are stored in the flash memory. And at paragraph [0067] of Cheline, it is indicated that the modem receives from a client computer upon requesting initiation of a VPN session a MAC address and/or IP address that is/are stored in the flash memory. Cheline's teaching to allow permanent memory to be written renders its VPN platform vulnerable to permanent infection and teaches away from what is recited in claim 55. Moreover, claims 55 and 56 are allowable for at least the other and further reasons stressed above with respect to claims 29, 30, 42 and 43.

In view of the foregoing, consideration and favorable action on all claims are respectfully requested. Accordingly, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Should any question remain in view of this communication, the Examiner is encouraged to call the undersigned so that a prompt disposition of this application can be achieved.

Respectfully submitted,

Scot A. Reader
Reg. Number 39,002
Tel. No. (303) 440-4050
Scot A. Reader, P.C.
1320 Pearl Street, Suite 228
Boulder, CO 80302